AMENDMENTS TO THE CLAIMS:

The following listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Cancelled).

2. (Currently amended) The ~~mobile telephone~~ handset according to claim 18, wherein the operating system controls the transmission of the IMEI to a mobile telephone operator by means of a secure OTA channel.

3. (Cancelled).

4. (Currently amended) The handset according to claim 18, wherein the ~~second data storage device~~ secure electronic module is a UICC.

5. (Currently amended) The handset according to claim 18, wherein the operating system controls the authentication of the ~~second data storage device~~ secure electronic module by the ~~first data storage device~~ storage support module.

6. (Currently amended) The handset according to claim 5, wherein the ~~second data storage device~~ secure electronic module and the ~~first data storage device~~ storage support module store encryption keys that are used to encrypt the secure communication channel.

7. (Currently amended) The handset according to claim 18, wherein the ~~second data storage device~~ secure electronic module blocks the use of the handset when a false IMEI is detected.

8. (Cancelled).

9. (Currently amended) The method of claim 19, wherein the ~~second data storage device also~~ secure electronic module transmits the IMEI to [[a]] the mobile telephone operator over a secure OTA channel.

10. (Previously presented) The method of claim 9, wherein the operator compares the IMEI with a black list of stolen handsets, and blocks the communications of the handset when the handset appears on the black list.

11. (Currently amended) The method of claim 19, wherein the ~~second data storage device~~ secure electronic module blocks the use of the handset when a false IMEI is detected.

12. (Currently amended) The handset according to claim 4, wherein the operating system controls the authentication of the ~~second data storage device~~ secure electronic module by the ~~first data storage device~~ storage support module.

13. (Currently amended) The handset according to claim 4, wherein the ~~second data storage device~~ secure electronic module blocks the use of the handset when a false IMEI is detected.

14. (Currently amended) The handset according to claim 5, wherein the ~~second data storage device~~ secure electronic module blocks the use of the handset when a false IMEI is detected.

15. (Currently amended) The handset according to claim 6, wherein the ~~second data storage device~~ secure electronic module blocks the use of the handset when a false IMEI is detected.

16. (Currently amended) The method of claim 9, wherein the ~~second data storage device~~ secure electronic module blocks the use of the handset when a false IMEI is detected.

17. (Currently amended) The method of claim 10, wherein the ~~second data storage device~~ secure electronic module blocks the use of the handset when a false IMEI is detected.

18. (Currently amended) A telephone handset, comprising:

a ~~first data storage device~~ storage support module storing an International Mobile Equipment Identity (IMEI) associated with an operator of a communication network and a first key;

a ~~second data storage device~~ secure electronic module storing a second key;

a processor;

a memory device including program instructions that, when executed by the processor, control the handset to:

authenticate, by the ~~second data storage device~~ secure electronic module, the ~~first data storage device~~ storage support module;

establish, ~~based on said authentication~~ in the event the secure electronic module determines that the storage support module is authentic, ~~an encrypted~~ a secure communication channel between the ~~first data storage device~~ storage support module and the ~~second data storage device~~ secure electronic module;

encrypt, by the storage support module, the IMEI using the first key;

transmit, via the ~~encrypted~~ secure communication channel, the encrypted IMEI from the ~~first data storage device~~ storage support module to the ~~second data storage device~~ secure electronic module; [[and]]

decrypt, by the secure electronic device, the encrypted IMEI received from the storage support module using the second key;

enable, by the secure electronic module, the handset to access the communication network ~~based on~~ in the event the secure electronic module determines that the decrypted IMEI received ~~by the second data storage device~~ from the storage support module is authentic; and

access, by the handset, the communication network using the authenticated IMEI, wherein the network grants access to the handset without further authentication of the authenticated IMEI.

19. (Currently amended) A method of securing a telephone handset, said method comprising:

authenticating a ~~first data storage device~~ storage support module by a ~~second data storage device~~ secure electronic module, said ~~first data storage device~~ storage support module

storing an International Mobile Equipment Identity (IMEI) associated with the operator of a communication network;

establishing, by a processor ~~based on said authentication~~ in the event the secure electronic module determines that the storage support module is authentic, ~~an encrypted~~ a secure communication channel between the ~~first data storage device~~ storage support module and the ~~second data storage device~~ secure electronic module;

encrypting, by the storage support module, the IMEI using a first key;

transmitting, ~~by the processor~~ via the ~~encrypted~~ secure communication channel, the encrypted IMEI from the ~~first data storage device~~ storage support module to the ~~second data storage device~~ secure electronic module; [[and]]

decrypting, by the secure electronic device, the encrypted IMEI received from the storage support module using a second key;

enabling, by the ~~processor~~ secure electronic module, the handset to access the communication network ~~based on~~ in the event the secure electronic module determines that the decrypted IMEI received ~~by the second data storage device~~ from the storage support module is authentic; and

accessing, by the handset, a communication network using the authenticated IMEI, wherein the network grants access to the handset without further authentication of the authenticated IMEI.

20. (New) A telephone handset, comprising:

a ~~first encrypted data storage device~~ storage support module storing an International Mobile Equipment Identity (IMEI) associated with the operator of a communication network and a first key;

a ~~second encrypted data storage device~~ secure electronic module storing a second key;

means for authenticating the ~~first data storage device~~ storage support module by the ~~second data storage device~~ secure electronic module;

means for establishing, ~~based on said authentication~~ in the event the means for authenticating determines that the storage support module is authentic, ~~an encrypted~~ a secure communication channel between the ~~first data storage device~~ storage support module and the ~~second data storage device~~ secure electronic module;

means for encrypting the IMEI using the first key;

means for transmitting, via the secure communication channel, [[an]] the IMEI from the ~~first data storage device~~ storage support module to the ~~second data storage device~~ secure electronic module; [[and]]

means for decrypting the encrypted IMEI received from the storage support module using the second key;

means for enabling the handset to access the communication network ~~based on~~ in the event the secure electronic module determines that the decrypted IMEI received by the ~~second data storage device~~ secure electronic module; and

means for accessing a communication network using the authenticated IMEI, wherein the network grants access to the handset without further authentication of the authenticated IMEI.